Ingénierie des exigences et conception des systèmes d'aéronefs

Patrice Micouin

▶ **To cite this version:**

Patrice Micouin. Ingénierie des exigences et conception des systèmes d'aéronefs. 5ème Conférence Annuelle d'Ingénierie Système (AFIS 2009), Sep 2009, PARIS, France. hal-00614129

HAL Id: hal-00614129
https://hal.science/hal-00614129

Submitted on 9 Aug 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

«Ingénierie des exigences et conception des systèmes d'aéronefs»

Dr Patrice MICOUIN
Laboratoire des Sciences de l'Information et des Systèmes
Arts et Metiers Paris'Tech,
2, cours des Arts et Métiers,
13100 Aix-en-Provence
patrice.micouin@incose.org

Résumé.

Le but de cet article est de proposer un cadre de conception des systèmes complexes aussi cohérent et complet que possible qui permette à la fois :
(1) d'intégrer les activités de développement et les activités d'évaluation de la sûreté,
(2) de satisfaire aux exigences émises par les autorités de certification telles que la l'EASA[1] et FAA[2],
(3) de répondre à des standards tels que l'ED-79/ARP 4754 [9], la ED-80/DO-254 [10], ou la ED-12/DO-178B [8],
(4) de préparer la voie à une ingénierie des systèmes aéronautiques basée sur des modèles qui est encore en cours d'élaboration.

Dans un premier temps, nous rappelons un certain nombre de résultats concernant l'ingénierie des exigences que nous avons publié dans un article [14] du « Journal of Systems Engineering » en 2008.

Dans un second temps, nous présentons les éléments architecturaux du processus d'ingénierie tel qu'il est présenté par le standard EIA-632 [3]. Nous l'adoptons comme cadre de notre travail.

Dans un troisième temps, nous montrons comment il est possible d'étendre le cadre proposé par l'EIA-632 pour y intégrer nos propositions relatives à l'ingénierie des exigences, et de rendre compte des différents attendus exprimés dans les réglementations et standards aéronautiques.

Introduction.

L'application démontrable du standard aéronautique ED-79/ARP 4754 tend à devenir un moyen de conformité à certaines exigences de certification émises par des organisations telles que l'EASA ou la FAA. Cependant, ce standard ne fournit pas de cadre strict de développement des systèmes d'aéronefs. Au contraire et sans doute pour conserver le plus de généralité possible il se réfère à un processus générique de développement assez sommaire décrit dans son annexe A.1[3]. Aussi se fait jour le besoin d'un cadre de développement qui vienne instancier ce processus générique de développement référencé dans l'ED-79/ARP 4754. Le présent article a pour but de répondre à ce besoin. Son second objectif est de franchir une étape supplémentaire dans la définition des processus d'une ingénierie des systèmes aéronefs basée sur les modèles (MBSE).

---

[1] **EASA** : European Aviation Safety Agency
[2] **FAA** : Federal Aviation Administration
[3] "*While there is no specific recommended process for systems development, a generic development model is described in Appendix A to assist in establishing common terminology and understanding. The specific development process selected should be described in sufficient detail to achieve mutual understanding of the key elements and their relationships*"(ARP 4754, 4.4.3 Development Plan)

1- Une théorie des exigences basées sur les propriétés.

Dans un article publié en 2008 dans le « journal of systems engineering », nous proposions une théorie des exigences basée sur la notion de propriété (Property Based Requirement).

Parmi les énoncés déontiques (c'est-à-dire les expressions qui énoncent une obligation ou une interdiction), que l'on rencontre dans une spécification, une distinction est introduite entre d'une part la notion d'attente (expression textuelle plus ou moins précise d'une demande d'une partie prenante) et d'autre part la notion d'exigence bien formée.

1-1 Définition des exigences bien formées.

Une exigence bien formée est définie comme une contrainte sur une propriété que possède un objet ou un ensemble d'objets lorsqu'une condition est satisfaite. Cette définition peut alors s'exprimer formellement de la manière suivante : when C $\Rightarrow$ val(O.P) $\subseteq$ D ce qui signifie : quand la condition C est réalisée, la propriété P de l'objet O doit se situer dans le domaine D (Pour l'interdiction, il suffit d'écrire when $C \Rightarrow val(O.P) \subseteq \bar{D}$ [$\bar{D}$ étant le complémentaire de D]).

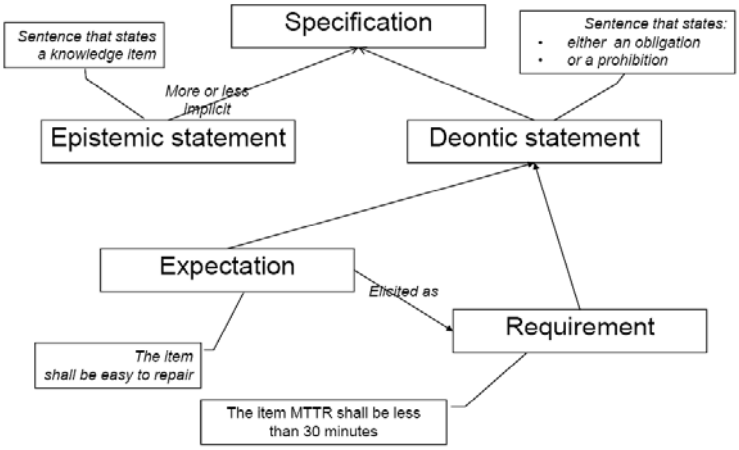

Figure 1. Exigences au sein d'une spécification.

Les objets dont il est question ici sont soit des entités physiques (objets *continuants*) conçues et réalisées par des humains à des fins définies soit des processus qui se déroulent au sein de ces mêmes entités physiques (objets *occurrents*[4]). Ces objets sont porteurs de propriétés multiples qui peuvent être classées en deux catégories : les propriétés structurelles d'une part et les propriétés comportementales de l'objet concerné. Un aéronef est, par exemple, un objet *continuant* caractérisé par ses propriétés structurelles (voilure fixe, voilure tournante, masse, etc.) et ses propriétés comportementales (caractéristiques de vol, autonomie, etc.). De même, un décollage ou un atterrissage de cet aéronef est un objet *occurrent* caractérisé par ses propriétés structurelles (ses phases, ses points caractéristiques) et ses propriétés comportementales (la séquence temporelle de ces phases et ses caractéristiques dynamiques).

Conséquence de notre définition des exigences bien formées, il existe au moins deux types d'exigences, les exigences structurelles qui concernent les propriétés structurelles de l'objet porteur et les exigences comportementales qui concernent ses propriétés comportementales. S'agissant, par exemple, d'un système embarqué fournissant les données air (ADC pour Air Data Computer) d'un aéronef (position verticale, vitesse verticale, ..), on peut poser sur lui des exigences structurelles de masse, d'encombrement, de forme, des exigences comportementales concernant le domaine de définition, la précision, le seuil de sensibilité des données fournies, la réponse à des signaux d'entrée caractéristiques (rampe, sinusoïde, ..).

Par exemple, le tableau ci-dessous exprime la précision requise sur l'altitude dans les conditions standards fournie par un ADC pour pouvoir être conforme au standard AS8002A [16].

[4] Les processus du cycle de vie sont aussi considérés comme des objets occurents qui se déroulent au sein d'objets continuants (équipe de projet, entreprises, équipage, etc.)

TABLE 1 - Altitude

Altitude Feet	Altitude Meters	Tolerance ± Feet	Tolerance ± Meters
0.	0.	25.	8.
1000.	305.	25.	8.
2000.	610.	25.	8.
3000.	914.	25.	8.
4000.	1219.	25.	8.
5000.	1524.	25.	8.
8000.	2438.	30.	9.
11000.	3353.	35.	11.
14000.	4267.	40.	12.
17000.	5182.	45.	14.
20000.	6096.	50.	15.
30000.	9144.	75.	23.
40000.	12192.	100.	30.
50000.	15240.	125.	38.

Tableau 1. Extrait du standard AS8002A relatif à la précision de l'information altitude.

Le type d'une exigence ne doit pas être confondu avec sa source qui est la partie prenante qui exprime l'exigence. Ainsi l'expression « exigence de certification » ne désigne pas un type d'exigence mais une source d'exigence, à savoir l'autorité de régulation.

De même, l'expression « exigence de sûreté » ne désigne pas non plus un type d'exigence mais une source d'exigence, à savoir ici une exigence résultant d'une évaluation de sûreté, étant entendu qu'une telle exigence de sûreté peut très bien être de nature structurelle ou de nature comportementale, voire une combinaison des deux. Par exemple, une exigence de sûreté qui imposerait à un système d'avoir une probabilité de défaillance inférieure à 10^{-9}/heure de vol est une exigence comportementale tandis qu'une exigence qui impose que l'architecture d'un système soit constituée de deux voies séparées et sans constituant de conception identique est une exigence structurelle.

En revanche, une exigence de performance peut être considérée comme une exigence comportementale.

Le processus d'élicitation (pour ce qui les concerne, les autorités parlent d'interprétation) est un processus permettant de passer d'une attente à une ou plusieurs exigences bien formées et nous faisons la conjecture que cette élicitation est en pratique toujours possible[5], même si elle peut s'avérer très compliquée. L'effort de standardisation aéronautique est un exemple (une « évidence ») de ce travail d'élicitation d'attentes formulées par les autorités de régulation qui conduit en pratique à l'expression d'exigences bien formées.

Dans ce travail d'élicitation, on rencontre très souvent des attentes et des exigences qui entretiennent entre elles des relations que nous avons désigné comme relations « *de dicto* », c'est-à-dire des relations purement linguistiques. Ainsi, l'attente « l'équipement fournissant la position verticale de l'aéronef devra être conforme à l'AC 29.1303 » entretient avec l'attente « l'équipement fournissant la position verticale de l'aéronef devra être conforme au TSO-C10b »[18] une relation « *de dicto* » dans la mesure où l'AC 29.1303 énonce que pour être conforme à la réglementation un altimètre sensitif doit être conforme au TSO-C10b. De même, l'attente « un ADC fournissant la position verticale de l'aéronef devra être conforme au TSO-C106 » entretient avec l'attente « un ADC fournissant la position verticale de l'aéronef devra être conforme au standard AS8002A » une relation « de dicto » dans la mesure où le TSO-C106 [19] énonce que pour être conforme un équipement doit être conforme à l'AS8002A.

[5] *Au demeurant, cette hypothèse n'a rien d'exorbitante, toutes les méthodes d'ingénierie, au travers d'acronymes tels que les TPM, MOE, MOP ou KPi font implicitement cette hypothèse qu'on peut relier à la célèbre formule de G. Bachelard tirée de « la formation de l'esprit scientifique » : « connaître, c'est mesurer ».*

Etant donné une exigence Ex, on peut définir l'ensemble SAT(Ex) des objets réellement possibles qui satisfont à cette exigence[6]. Par exemple, on peut s'intéresser à l'ensemble des systèmes ADC qui sont conformes au standard AS8002A. Cet ensemble peut être désigné par SAT(AS8002A).

Cet ensemble SAT(Ex) est intéressant parce qu'il permet de définir deux relations entre exigences: une relation d'ordre « *être plus contraignante que*» et une opération de composition entre exigences.

1. Nous dirons qu'une exigence Ex-1 *est plus contraignante* qu'une exigence Ex-2 si et seulement si l'ensemble SAT (Ex-1) est un sous ensemble SAT(Ex-2) i.e. Ex-2$\leq$Ex-1$\Leftrightarrow$SAT(Ex-1)$\subseteq$SAT(Ex-2).
2. D'autre part nous dirons que l'exigence Ex *est la composée* de Ex-1 et Ex-2 si et seulement si SAT(Ex) = SAT(Ex-1) $\cap$ SAT(Ex-2) et on note alors Ex=Ex-1$\wedge$Ex-2.

Par exemple on peut s'intéresser d'une part à l'ensemble des systèmes ADC conformes à l'AS8002A SAT(AS8002A) et d'autre part à l'ensemble SAT(ARINC706-4) des systèmes ADS qui sont conformes à la caractéristique ARINC 706-4 [5]. On pourra dire que l'ensemble des exigences tirées de ARINC 706-4 est plus contraignant que celles tirées de AS8002A si et seulement si SAT(ARINC706-4)$\subseteq$SAT(ARINC706-4)

Mathématiquement parlant, on peut montrer que l'ensemble des exigences portées par un système a une structure de semi-treillis et que la relation « être plus contraignante que» et l'opérateur de composition entre exigences s'engendrent mutuellement.

Il existe donc finalement trois types d'exigences, les exigences structurelles, les exigences comportementales et les exigences mixtes qui sont des composées d'exigences structurelles et comportementales. Les exigences d'interface sont un cas typique d'exigences mixtes qui combinent à la fois des exigences structurelles (nombre de connecteurs, dimensions, forme, ..) et des exigences comportementales (temporisation, protocoles, ..). Un exemple classique dans le domaine aéronautique d'exigence mixte est le suivant « l'ensemble des sorties d'un système X devra être conforme à la spécification ARINC 429 » [4] fait référence à un ensemble d'exigences structurelles (mécaniques, électriques) et comportementales (protocoles, débits, typage des messages) dont la composition définit l'exigence « doit être conforme à l'ARINC 429 ».

Il faut aussi noter que les exigences bien formées concernant un même objet sont rarement indépendantes les unes des autres parce qu'elles contraignent des propriétés qui sont elles mêmes dépendantes les unes des autres (par exemple, certaines propriétés structurelles peuvent directement conditionner des propriétés comportementales). Nous disons que de tels exigences sont couplées et ne peuvent être définies indépendamment sous peine d'introduire des incompatibilités (le système n'est pas faisable). On a notamment de nombreux couplages entre des exigences portant sur des grandeurs liées entre elles par des lois physiques. Imposer une contrainte (exigence) sur l'une d'entre elles, c'est forcément limiter les degrés de liberté des autres grandeurs qui lui sont liées physiquement par une loi. Par opposition aux relations que nous avons appelé précédemment « *de dicto* », les relations de couplage entre exigences sont des relations « *de re* », dans la mesure où le couplage n'est pas un effet du langage (« *de dicto* ») mais un effet de la réalité matérielle (« de re ») qui lie les propriétés des objets et ce, indépendamment du langage. Si l'on considère par exemple *la* position verticale et la vitesse verticale d'un aéronef délivrée par un ADC, ces deux grandeurs sont liées entre elles physiquement, la seconde étant la dérivée par rapport au temps de la première.

1-2 Operations sur les exigences bien formées.

Selon l'ED-79/ARP 4754, il convient, de manière itérative, (1) de définir les exigences applicables au système à développer et (2) de les valider, c'est-à-dire de s'assurer qu'elles sont suffisamment complètes (il n'en manque pas d'essentielles) et qu'elles sont correctes. Les exigences étant validées, il convient de (3) concevoir de manière l'architecture d'un système-solution c'est-à-dire un ensemble de produits en interaction qui pris ensemble satisfont aux exigences du système. L'assurance que le système réalisé répond bien à ses exigences est obtenu grâce (4) au processus de vérification du système par rapport à ses exigences ce qui peut être obtenu à l'aide d'essais, d'analyses et de preuves…

Sur la base théorique rapidement présentée ci-dessus, on peut définir un ensemble d'opérations associées aux exigences. Ces opérations sont au nombre de six et concernent (1) la génération des

[6] *Cet ensemble peut éventuellement vide, ce qui signifie que l'exigence correspondante est hors d'atteinte.*

exigences, (2) la dérivation, (3) la validation des exigences, (4) la vérification par rapport à des exigences, (5) la modification et (6) la suppression d'exigences.

Une exigence bien formée a trois origines possibles : généralement une exigence bien formée résulte d'un processus d'élicitation à partir d'attentes de parties prenantes mais elle peut également être exprimée « ex-nihilo » par une partie prenante. Enfin la troisième voie d'engendrement est la dérivation d'exigences que nous discuterons ci-dessous.

(1) L'élicitation d'une attente en un ensemble d'exigences bien formées peut s'avérer être un processus extrêmement complexe et long. Un cas particulièrement remarquable concerne la formulation de certaines attentes que l'on trouve dans les spécifications de certification émises par l'EASA ou la FAA. Certaines formulations sont tellement ouvertes et générales pour pouvoir s'adapter à la diversité des situations qu'elles ont nécessité la production d'un matériel interprétatif important pour rendre possible la vérification de la conformité à de telles attentes. Ce matériel interprétatif des réglementations constitue un corpus imposant d'« *Advisory Circular* » (ACs) pour la FAA et d'« *Acceptable Means of Compliance* » (AMCs) pour l'EASA qui s'est développé au fil des ans pour fournir une interprétation réputée correcte des exigences de certification, fixer des définitions non ambigües et pour proposer des moyens acceptables pour établir la conformité d'un système aux exigences de certification qui lui sont applicables.

(2) La notion d'exigence dérivée connait des interprétations contradictoires. Celle que nous développons ici est, selon nous, identique à celle développée par exemple dans l'ARP 4761 [11] (à propos des exigences dérivées de sûreté), celle de l'EIA 632 et encore celle défendue par Scott Jackson dans son ouvrage « *Systems engineering for commercial aircraft* » [13]. La dérivation d'une exigence est une transformation qui substitue un ensemble d'exigences de niveau sous systèmes à une exigence de niveau système moyennant un ensemble d'hypothèses concernant une décomposition décidée d'un produit en sous-systèmes. La dérivation est donc une opération conditionnelle qui ne vaut que si les hypothèses de conception restent valides. Plusieurs exemples de dérivation sont donnés dans l'ED-79/ARP 4754 notamment celui-ci. Un système S doit être DAL A (EX-S : S.DAL=A). Supposons que le choix de conception CC suivant est fait : le système S est constitué de deux portions P et B indépendantes et dissimilaires, B fonctionne en parallèle à P et le redonde. Alors pour la portion P on obtient l'exigence dérivée suivante EX-P : P.DAL=A et pour la portion B, on obtient l'exigence dérivée suivante EX-B : B.DAL≥C. On peut dans ce cas particulier, formaliser l'opération de dérivation de la manière suivante : $S.DAL=A \wedge CC \Rightarrow P.DAL=A \wedge B.DAL\geq C$. De manière générale, l'opération de dérivation remplace une exigence donnée par des exigences dérivées qui prises isolement peuvent être moins contraignantes que l'exigence de départ mais qui prises ensemble sont plus contraignantes que l'exigence de départ.

(3) Ce second point nous amène naturellement à la question de la validation des exigences et des hypothèses. L'ED-79/ARP 4754 indique que la validation des exigences consiste à s'assurer qu'elles sont suffisamment complètes et correctes et qu'elle devrait être menée étape par étape du plus haut niveau de spécification du système vers ses niveaux les plus bas. Nous reformulons cette caractérisation de la manière suivante : Soit S un ensemble de systèmes techniques qu'on désire développer, par exemple un ensemble d'aéronefs ayant le même certificat de type (TC). Soit {Ex} un ensemble d'exigences bien formées, l'ensemble {Ex} constitue une spécification valide de S si et seulement si SAT({Ex})=S.
    a. Valider l'ensemble des exigences {Ex}, c'est essayer de s'assurer, par avance, que SAT({Ex})=S.
    b. Si $SAT(\{Ex\}) \subset S$ alors {Ex} sur-spécifie S. Il y a « trop » d'exigences ou elles sont trop contraignantes pour l'ensemble de systèmes visé. La spécification écarte des systèmes qui seraient acceptables.
    c. Si $S \subset SAT(\{Ex\})$ alors {Ex} sous-spécifie S. Il manque des exigences ou elles ne sont pas assez contraignantes pour l'ensemble de systèmes visé. La spécification conserve des systèmes qui ne sont pas acceptables.

    La validation des exigences a donc pour but de s'assurer que le juste besoin a été spécifié et elle requière la mise en œuvre de diverses méthodes incluant l'expérience acquise en service, les jugements d'experts, les analyses, la simulation et les essais.

(4) La vérification d'un système réalisé S_R par rapport à des exigences {Ex} consiste à démontrer que le système réalisé est bien conforme aux exigences spécifiées c'est-à-dire que $S_R \in SAT(\{Ex\})$. La vérification du système par rapport à ses exigences requière la mise en œuvre de diverses méthodes incluant l'inspection, l'audit, les analyses et les essais.

(5) et (6) La modification et la suppression d'exigences posent la question du couplage entre exigences. On ne peut impunément modifier ou supprimer une exigence sans que cela ait un impact sur les exigences qui lui sont couplées. C'est particulièrement vrai lorsqu'on remplace une exigence par une exigence moins contraignante. Les exigences qui lui sont couplées peuvent devenir impossibles à satisfaire.

2- L'ANSI/EIA-632.

L'EIA 632 « *Processes for Engineering a System* » est un standard conçu pour conduire le développement de systèmes techniques. Sa version la plus récente date de septembre 2003. Le standard propose essentiellement deux choses : d'une part un cadre conceptuel qui permet de décrire ce qu'est un système technique et d'autre part un ensemble d'activités et de processus qui permettent de conduire l'ingénierie d'un système tel que défini précédemment. Dans les deux sections suivantes nous présentons d'une part le cadre conceptuel qui permet de décrire un système technique et d'autre part les processus qui permettent d'en faire l'ingénierie.

2-1 Les systèmes selon l'EIA-632.

Selon l'EIA 632, un système se présente comme un arbre constitué d'un nombre quelconque de blocs de construction (Building blocks) comme illustré sur la figure 2 ci-dessous. Chaque bloc de construction présente la même structure, où qu'il soit placé dans l'arbre. Le bloc racine de l'arbre à la même structure que n'importe quel nœud de l'arbre.

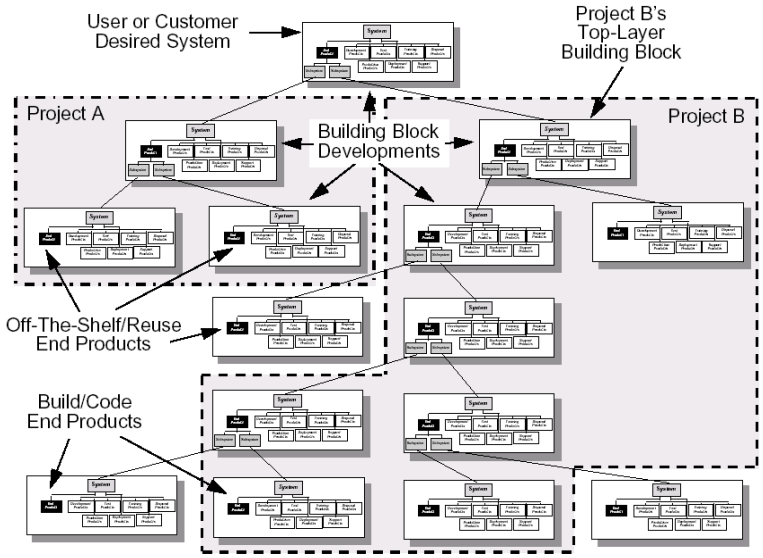

Figure 2. Arbre système

Cette structure de bloc est présentée sur la figure 3 et décrit un système comme étant constitué de produits de deux sortes : les produits opérationnels (ou finals) qui réalisent les fonctions opérationnelles du système et les produits support (enabling) qui permettent d'assurer les fonctions de support du système, c'est-à-dire les processus du cycle de vie du système. Chaque produit (final ou support) peut être soit directement construit/codé/pris sur étagère, soit faire l'objet, à son tour, d'une décomposition en sous systèmes qui donneront naissance à de nouveaux blocs de construction.

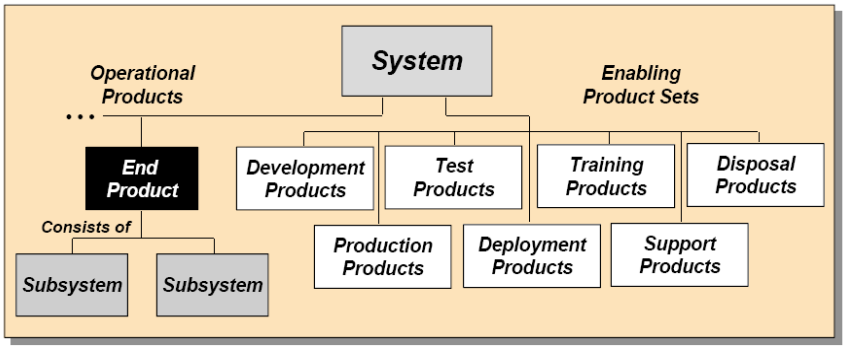

Figure 3. Bloc de construction

Ainsi un système aéronef ne se réduit pas au seul produit aéronef mais inclut également les produits de développement, de production, d'essais, ses produits d'entraînement et de maintenance associés.

Cette vision d'un système appelle plusieurs commentaires :

On peut tout d'abord souligner qu'il s'agit d'une construction répétitive menée à une profondeur non définie par avance mais répétée autant de fois que nécessaire (par opposition à celle présentée par l'IEEE 1220 limitée à cinq niveaux ou encore comparée avec les quatre niveaux de l'ED-79/ARP 4754 : aéronef, système, item, HW/SW).
On peut également remarquer une égalité de traitement entre les produits opérationnels et les produits de support. Le bloc de construction est donc un cadre d'ingénierie simultanée où l'on considère de manière concomitante le produit opérationnel (comme un aéronef) et ses produits support comme ses moyens de développement, de production, ses moyens de maintenance, ses moyens de formation (simulateurs) et également ses moyens de démantèlement.

Enfin, on pourrait croire que les processus et/ou les humains sont en dehors de la boucle, oubliés hors du système. En fait, cette appréciation est inexacte dans la mesure où les produits de support correspondent aux moyens avec lesquels les operateurs auront à conduire les processus du cycle de vie du système, comme par exemple, un simulateur d'entrainement, d'un manuel de vol ou d'un manuel de maintenance, dédiés à la formation et à l'assistance du pilote ou du mécanicien. Le parti-pris de ne représenter que les produits ne signifient donc pas que les processus et les humains ont été oubliés.

2-2 Les processus d'ingénierie selon l'EIA-632.

L'EIA 632 identifie treize processus qui sont à appliquer sur chaque bloc de construction du système

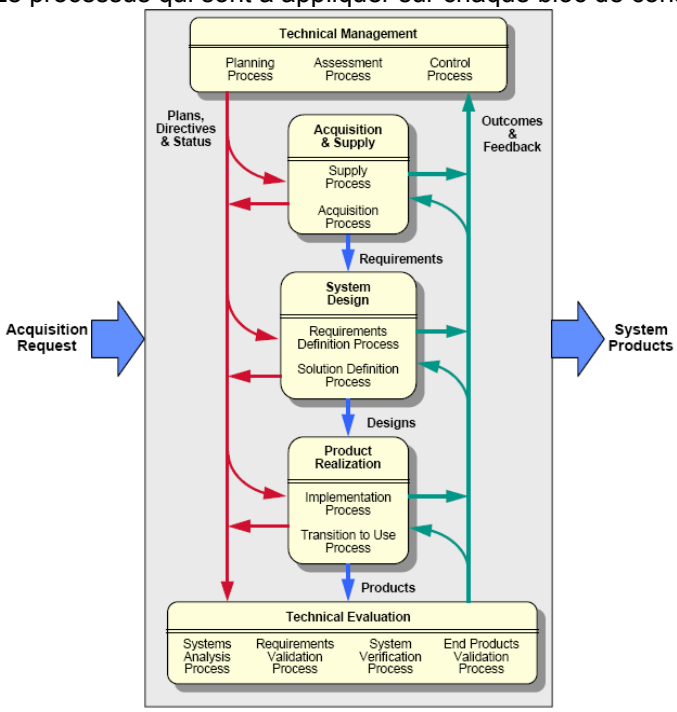

Figure 4. Processus pour l'ingénierie d'un système

Compte tenu des limites de cet article nous ne nous focaliserons que sur quatre d'entre eux : (1) la définition des exigences, (2) la validation des exigences, (3) la définition de la solution et (4) la vérification du système. Ces quatre processus font écho à des processus similaires identifiés dans l'ED-79/ARP 4754 lequel constitue le standard de développement des systèmes complexes aéronautiques.

2-3 La conception système selon l'EIA-632.

L'EIA 632 reprend les mêmes processus que ceux évoqués ci-dessus, tout en apportant une formalisation beaucoup plus stricte.

La figure 5 suivante donne une représentation de ces processus en introduisant de nouveaux concepts. Il s'agit essentiellement des notions, de représentations logiques et physiques, d'exigences dérivées et de solution de conception. Confronté à un ensemble d'exigences validées, le(s) concepteur(s) du système va (vont) imaginer une (ou des) solution(s) logique(s), c'est-à-dire un (ou plusieurs) modèle(s) de solution logique (la neutralité du terme logique a été choisie

intentionnellement pour laisser la place à différents types de modélisation possibles tout en soulignant qu'il ne s'agit pas de représentation physique).

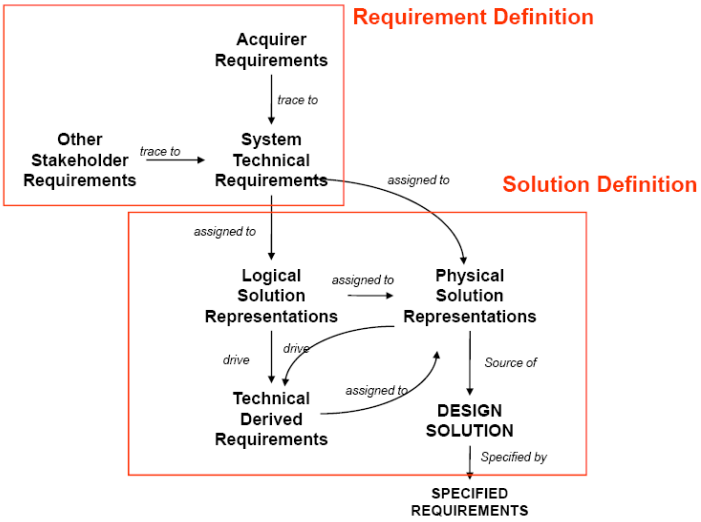

Figure 5. Conception d'un système selon l'EIA 632.

Un des modes de représentation logique possible est la modélisation fonctionnelle qui permet de définir des chaînes fonctionnelles articulées les unes aux autres en une architecture fonctionnelle. Elles peuvent être associées à des représentations du type diagrammes d'états. Le modèle conceptuel de données constitue un autre mode de représentation disponible pour modéliser les données internes ou échangées aux interfaces. Mais des modes de représentations alternatifs peuvent également être envisagés.

Quand de tels modèles de solution logique ont été identifiés, il devient possible d'allouer certaines exigences du système à ces modèles et de les transformer en exigences dérivées allouées à différents éléments de la solution logique. Une exigence comportementale pourra être ainsi allouée à une chaîne fonctionnelle et transformée en exigences dérivées allouées aux différents maillons de la chaîne.

La figure 6, ci-dessous, donne un exemple sommaire de conception logique possible d'une exigence comportementale d'une avionique : « Fournir l'altitude ».

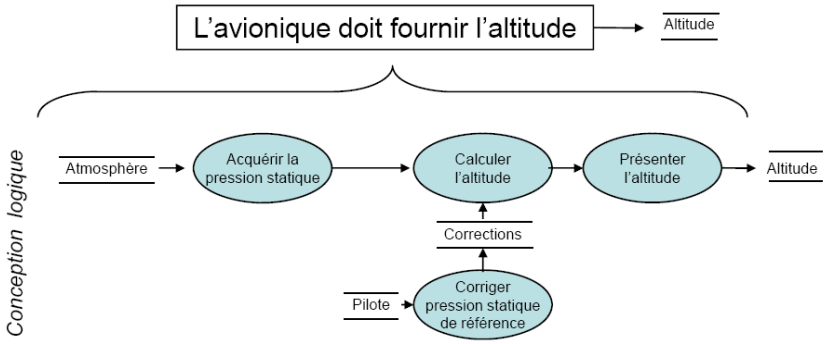

Figure 6. Conception fonctionnelle d'une chaîne fournissant l'altitude..

Une fois imaginés le ou les modèles de solution logique, l'EIA 632 propose de définir un ou des modèles de solution physique. Les éléments de solution logique sont alloués à des éléments de solution physique qu'ils matérialisent. Les exigences dérivées allouées aux éléments de solution logique sont alors, de facto, allouées aux éléments physiques qui les matérialisent. Certaines exigences du système, parce qu'elles n'étaient pas pertinentes au niveau logique (on pense, par exemple, à des exigences de masse, de forme ou de volume) sont directement allouées aux modèles physiques et dérivées en exigences allouées à des éléments de ces modèles physiques.

La figure 7, ci-dessous, donne un exemple sommaire d'une conception physique possible correspondant à la conception logique précédente :

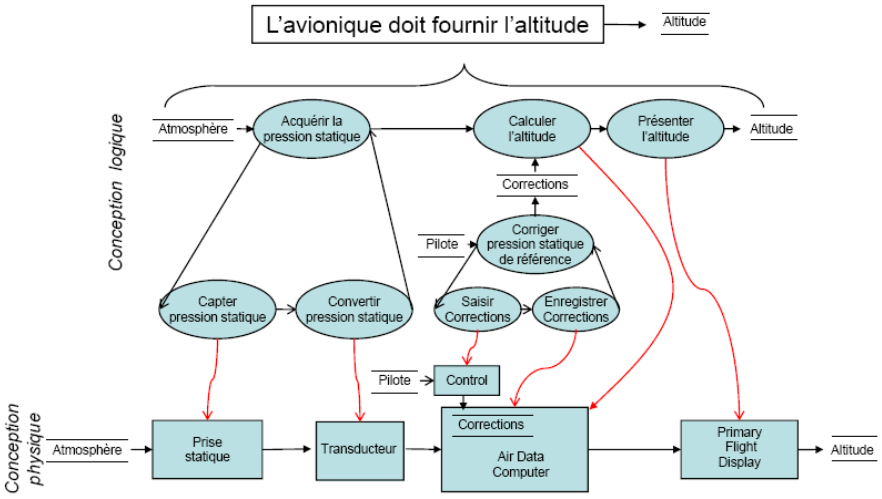

Figure 7. Conception physique d'une chaîne fournissant l'altitude..

Le résultat de ces processus de conception et de dérivation/allocation des exigences constitue une solution de conception. Une solution de conception correspond à différents ensembles d'exigences spécifiées. Certains peuvent être utilisés pour fabriquer ou coder des produits constitutifs de la solution, d'autres pour acquérir de tels produits et enfin d'autres encore, concernent les sous systèmes de produits à développer. La figure 8, ci-dessous, donne une représentation des exigences spécifiées qui résultent de la conception d'un bloc de construction.

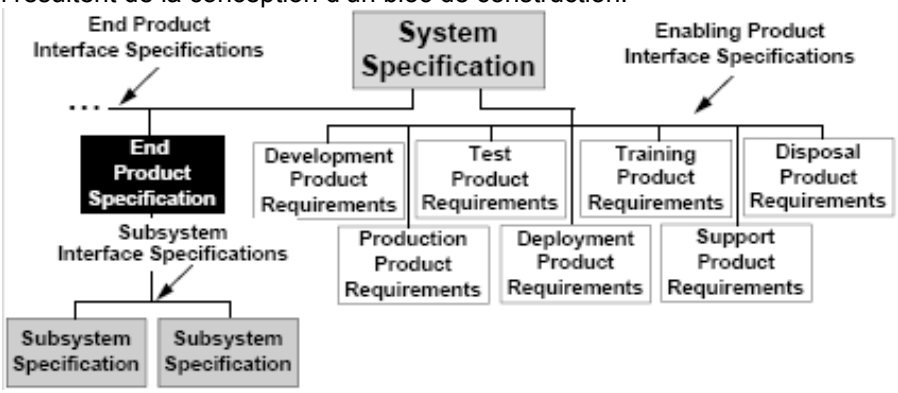

Figure 8. Exigences spécifiées résultant de la conception d'un bloc.

Cette vision de la conception système est conforme à l'architecture générale des systèmes techniques selon l'EIA 632, puisqu'il peut être répété de façon systématique pour chaque bloc de construction. Le processus de conception système s'arrête lorsqu'il est possible d'acquérir, de construire ou de coder tous les produits identifiés.

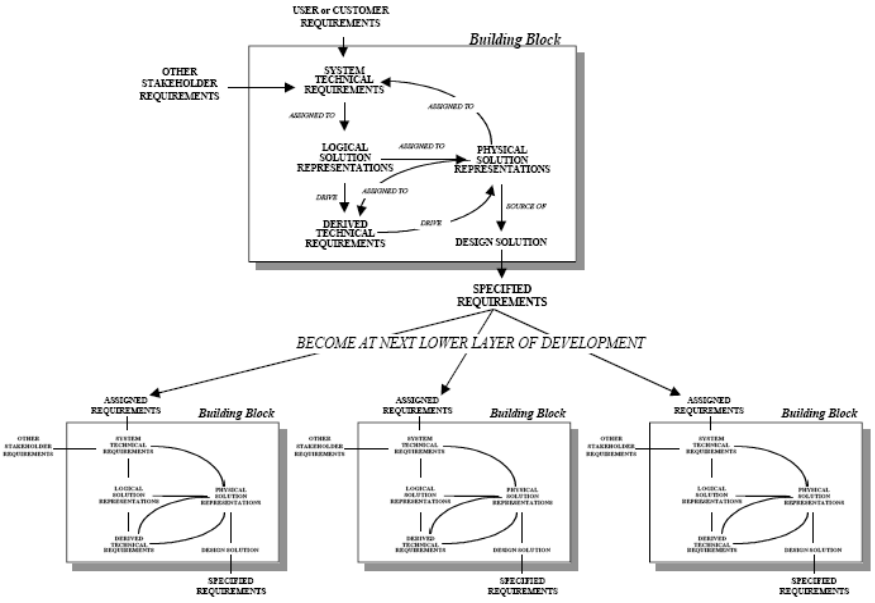

Figure 9. Enchainement de processus de conception selon l'EIA 632.

Pour des présentations plus complètes de l'EIA 632, on peut consulter, par exemple, le chapitre 1 de l'ouvrage « *Avionics, development and implementation* » [17], rédigé par James N. Martin (The Aerospace Corporation), qui est l'un des maîtres d'œuvre du standard. On pourra également plus directement se reporter au standard lui-même.

2-4 Validation des les exigences bien formées dans le cadre de l'EIA-632.

Lorsqu'on applique un processus de conception conforme à l'EIA 632, les exigences spécifiées à l'issue de la conception d'un bloc de construction résultent de la dérivation des exigences techniques du système.

Ce que nous avons indiqué ci-dessus au § 1-2 (3) concernant la validation des exigences s'applique donc particulièrement bien aux exigences dérivées. En effet, pour affirmer qu'un ensemble d'exigences dérivées est validé, il convient d'établir que la conjonction de ces exigences est au moins aussi contraignante que l'exigence dont elles sont issues ou encore SAT(Exigences specifiées) $\subseteq$SAT (Exigences techniques du système).

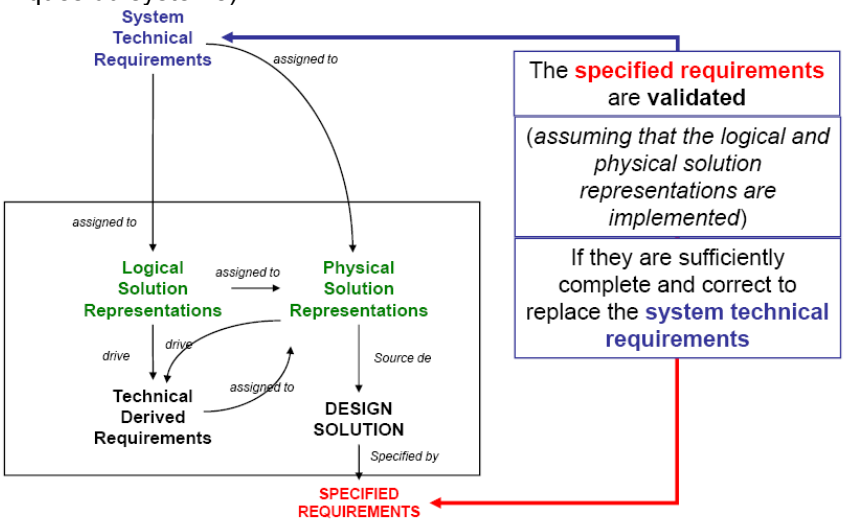

Figure 10. Validation des exigences dérivées.

Si l'on suppose, sur la figure 10, que les exigences techniques du système sont validées alors les exigences spécifiées issues du processus de conception du bloc de construction seront également validées s'il est possible d'établir par analyse que ces dernières prises ensemble sont au moins aussi contraignantes que les exigences dont elles sont issues (sous l'hypothèse que les choix de conception effectués seront effectivement réalisés).

Exemple simple, pour montrer que les exigences de masse allouées aux constituants d'un système sont valides il suffit de montrer que la somme des masses exigées est inférieure à la masse exigée du système. De même, pour le pire temps d'exécution d'un processus constitués de différents sous processus.

Les exigences techniques du système sont elles mêmes validées si elles dérivent elles mêmes entièrement des exigences techniques d'un système englobant. Dans le cas contraire, si des exigences d'autres parties prenantes ont été injectées ou s'il s'agit du système de plus au niveau alors la validation de ces exigences nécessite un recours à des moyens classiques : validation par les acquéreurs, simulations, jugements d'experts, analyses, expérience en service, essais, etc

2-5 Vérification des systèmes par rapport aux exigences dans le cadre de l'EIA-632.

Dans le cadre de l'EIA 632, La vérification d'un système réalisé S_R à partir de sous systèmes SS_R assemblés physiquement et fonctionnellement consiste alors en

1. la vérification des sous systèmes réalisés par rapport aux exigences qui leur ont été spécifiées.
2. La vérification de la conformité de l'intégration des sous systèmes réalisés par rapport à la description de conception.
3. la vérification du système réalisé par rapport aux exigences techniques du système.

Cette vérification est illustrée sur la figure 11, ci-dessous.

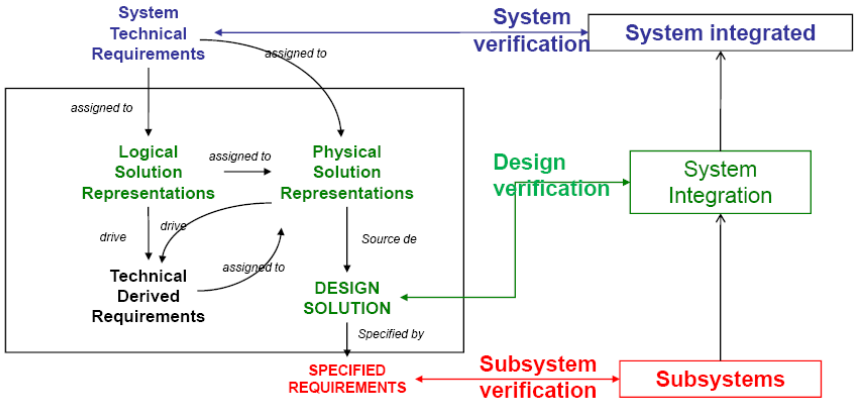

Figure 11. Vérification par rapport aux exigences.

La vérification du système par rapport à ses exigences requière divers moyens incluant l'inspection, l'audit, les analyses et les essais.

3- Les exigences de certification.

Les exigences de certification sont des exigences consignées dans des spécifications de certification, comme par exemple, la CS 29 [7] pour les hélicoptères lourds. Les avionneurs, lorsqu'ils veulent mettre un nouveau produit sur le marché, doivent faire la démonstration auprès des autorités que ce produit répond aux exigences de certification qui lui sont applicables. Certaines exigences de certification concernent des capacités particulières du produit, il s'agit d'exigences spécifiques, d'autres s'appliquent à tous les systèmes d'un aéronef, il s'agit d'exigences générales.

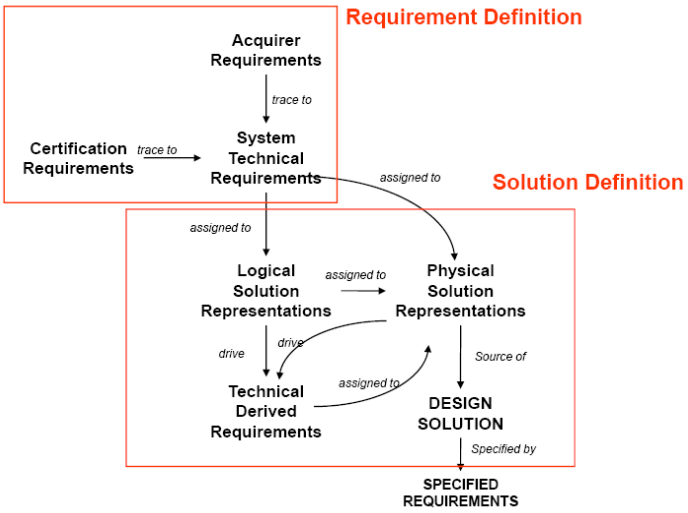

Figure 12. Prise en compte des exigences spécifiques de certification

Comme exemple d'exigence spécifique, on peut citer la CS29.1303 qui impose que chaque position de pilotage dispose d'un ensemble défini d'instruments de vol et de navigation tel qu'un altimètre sensitif (i.e capable d'enregistrer de faibles écarts d'altitude) ou un variomètre[7]. La formulation fait parfois une référence implicite à une technologie donnée (éventuellement datée), ce qui a amené à un travail d'interprétation (élicitation) car ce qui est requis c'est que soit fournie l'information position verticale par rapport à une référence (niveau de la mer, par rapport à un point au sol) et sa dérivée, la vitesse verticale dans des conditions de précision déterminées dans des contextes d'emploi variés et non l'utilisation d'une technologie donnée. Ce travail d'interprétation se retrouve dans l'AC 29-2C où sont indiquées indirectement[8] les exigences à satisfaire pour la mise à disposition des informations position et vitesse verticales. De telles exigences spécifiques s'intègrent assez naturellement au processus général de développement proposé par l'EIA 632 sans qu'il soit besoin d'apporter des aménagements particuliers pour en rendre compte. Ainsi, la fourniture de l'information position verticale nécessite l'introduction d'une chaine fonctionnelle (exploitant un principe physique) qui permette d'acquérir la position verticale de l'appareil et de la présenter aux positions de pilotage après

[7] *CS 29.1303 Flight and navigation instruments : The following are required flight and navigational instruments: (a) .. (b) A sensitive altimeter. .. (i) A rate-of-climb (vertical speed) indicator…*

[8] Reference à l'AC 25-11 qui lui-même fait reference à l'AS 8002.

différents traitements intermédiaires. Partant de connaissances sur la physique de l'atmosphère, la baro-altimétrie exploite la variation de la pression atmosphérique en fonction de l'altitude. D'autres principes physiques peuvent être également mis en œuvre dans certaines, voir toutes, les phases du vol. Ainsi, l'altimétrie radar exploite la réflexion et le temps de propagation des ondes radar, les systèmes inertiels de navigation les propriétés inertielles des solides en rotation, les systèmes de localisation des principes de triangulation.

Nous avons déjà représenté sur la figure 6, une chaîne fonctionnelle qui permet de déterminer la position verticale d'un aéronef à partir de la pression statique.

Sur la figure 7, nous avons représenté les éléments d'une chaîne physique constitué de capteurs, des unités de traitement et des afficheurs choisis dans un catalogue des solutions physiques éprouvées ou innovantes permettant de doter le système de la propriété attendue. La conformité de cette solution à l'exigence de certification de départ pourra se faire à l'occasion d'essais en vol précédés d'essais sol et en laboratoire.

En revanche, il n'en va pas tout à fait de même pour ce qui concerne les exigences générales de certification qui font l'objet du paragraphe suivant.

4- Les exigences de sûreté (safety).

Certaines exigences de certification, identifiées par les ACs ou les AMCs comme générales, sont applicables à n'importe quel système d'aéronef. Un exemple d'exigence générale est fourni par la CS29.1309 qui prescrit que les systèmes doivent être conçus de telle sorte que l'occurrence d'un cas de défaillance qui interdirait la poursuite d'un vol en sécurité doit être extrêmement improbable[9].

Montrer la conformité d'un système aéronautique à une telle exigence a nécessité le développement un important matériel interprétatif (AC29.1309) permettant d'une part de fixer des définitions (failure condition, continued safe flight and landing, extremely improbable) partagées par tous et d'autre part de convenir de moyens permettant de montrer la conformité à cette exigence.

Il est ainsi recommandé de conduire une évaluation fonctionnelle des risques (FHA) tant au niveau aéronef qu'au niveau de ses systèmes, de mener des évaluations de sûreté des systèmes (SSA) en conduisant des processus qui préfigurent ceux recommandés par l'ED-79/ARP 4754. La recommandation ED-79/ARP 4754 devient donc pratiquement un moyen acceptable pour démontrer la conformité à cette exigence, tandis que les standards ED-80/DO-254 et ED-12/DO-178B se sont imposés comme moyens de conformité au niveau plus spécifiques des composants électroniques complexes (CEH) et des logiciels embarqués.

Pour une présentation synthétique de ces différents standards aéronautique, on peut consulter, par exemple, le chapitre 3 de « *Civil Avionics Avionics* » de I. Moir et A. Seabridge **[15]**.

Considérées sous cet angle, les exigences de sûreté apparaissent alors comme des exigences dérivées d'exigences de certification.

Les systèmes d'aéronefs permettant de satisfaire à l'exigence CS29.1303 et donc en particulier de fournir au(x) pilote(s) l'information de position et de vitesse verticales doivent donc être conçus de telle sorte que leur probabilité de défaillance soit inférieure à 10^{-9} par heure de vol s'ils peuvent connaître des cas de défaillance catastrophiques. Pour se conformer à une telle exigence, l'ARP 4754 recommande notamment de mettre en œuvre un processus d'évaluation de la sûreté cohérent avec le processus de développement. C'est ce que nous nous proposons de faire dans ce qui suit par une extension du modèle de conception proposé par l'EAI 632.

En effet, l'intégration des processus d'évaluation de la sûreté nécessite une extension du modèle de conception proposé par l'EIA 632 (ce modèle a été représenté sur la figure 5).

La conception d'un bloc de construction répondant à des exigences de sûreté requiert deux sortes de modification illustrées sur la figure 13:

[9] CS 29.1309 Equipment, systems, and installations
(b) The rotorcraft systems and associated components, considered separately and in relation to other systems, must be designed so that - (2) For Category A rotorcraft: (i) The occurrence of any failure condition which would prevent the continued safe flight and landing of the rotorcraft is extremely improbable; and (..)

(1) une modification du processus de définition des exigences et

(2) une modification du processus de définition de la solution.

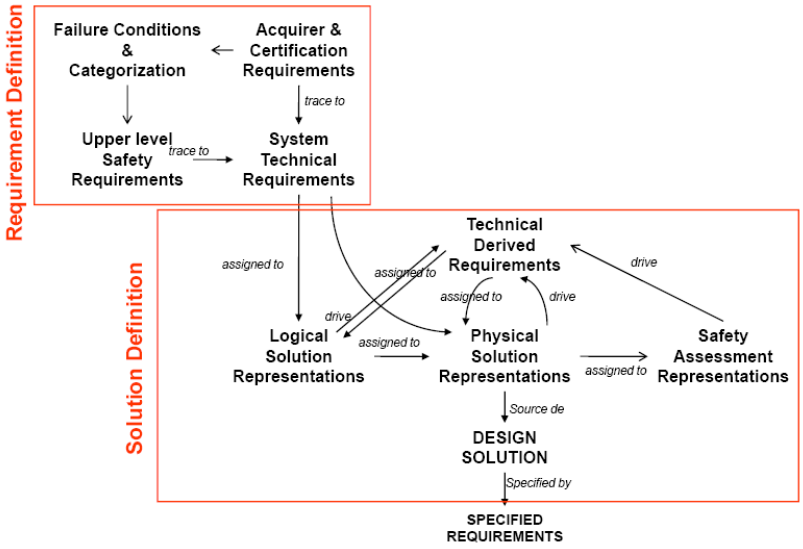

Figure 13. Prise en compte des exigences de sûreté

(1) En ce qui concerne le processus de définition des exigences techniques d'un bloc de construction, une évaluation fonctionnelle des risques (FHA) doit être menée. Elle prend en compte les exigences comportementales attendues par l'acquéreur et l'autorité de certification afin de déterminer les cas de défaillance (failure condition). Comme le recommande l'ED-79/ARP 4754, ces cas de défaillance sont classés en fonction de la sévérité de leurs effets (catastrophique, dangereux, ..). Des objectifs et des exigences de sûreté de haut niveau sont alors alloués au système, en fonction de la sévérité de ces cas de défaillances

Pour reprendre nos exemples, quelles pourraient être les conséquences (relativement à une poursuite du vol en sécurité) de la perte pour le(s) pilote(s) de l'information altitude ou vitesse verticale ? Quelles pourraient être les conséquences de la présentation aux pilotes d'une information altitude ou vitesse verticale erronées. Comme le souligne l'AC 25.11 [1], l'information altitude erronée ou perdue pour le(s) pilote(s) lors d'un vol sans visibilité (IMC) sont considérées comme catastrophiques.

Il en résulte que des exigences de sûreté comme :

a. La conception du système fournissant l'indication de position verticale devra être à sécurité intégrée (fail safe design),
b. La probabilité de défaillance du système fournissant l'indication de position verticale devra être inférieure à 10^{-9} par heure de vol.
c. Le niveau d'assurance de développement (S. DAL) du système est A

soient des conséquence de cette analyse (FHA)[10].

(2) En ce qui concerne le processus de définition de la solution d'un bloc de construction, une évaluation préliminaire de la sûreté du système (PSSA) est menée pour allouer aux éléments de la solution logique et de la solution physique les exigences de sûreté dérivées des exigences de sûreté de haut niveau. Cette dérivation des exigences de sûreté s'appuie sur un troisième type de modélisation complémentaire des modélisations précédentes (logiques et physiques), il s'agit de modélisation d'évaluation de la sûreté comme les diagrammes de fiabilité (dependability diagrams, DD), les arbres de défaut (FTA), ou les chaînes de Markov.

Cette modélisation est dépendante des choix de conception logiques et physiques.On notera même qu'il existe une transformation pratiquement directe d'une représentation d'architecture physique en diagramme de fiabilité (DD) et une transformation tout aussi directe vers l'arbre de défaillance correspondant.

[10] Conformes à l'ARP 4754 Table 5.

Ces éléments de modélisation supportent la dérivation des exigences de sûreté en phase de conception tandis qu'ils permettront de supporter les évaluations de sûreté (SSA) en phase de vérification (voir figure 17).

Ces modèles d'évaluation de la sûreté permettent également de supporter les analyses de cause commune (CCA), tandis que des modèles physiques (géographiques) permettent de supporter des analyses de sûreté de zones (ZSA).

Pour poursuivre nos exemples, l'exigence de conception à sécurité intégrée (fail safe) impose à l'architecte du système fournissant l'indication de position verticale d'introduire un niveau de redondance suffisant. Les éléments redondants devront alors faire l'objet d'une partition (ségrégation logique et au besoin physique) destinée à prévenir une dissémination de fautes d'une partition à une autre.

Enfin, les partitions pourront faire l'objet de conceptions dissimilaires pour prévenir les fautes dues aux erreurs de conception. Le tableau 4 de l'ARP 4754 nous fournit des exemples d'architecture types (design patterns) susceptibles de rendre extrêmement improbables des cas de défaillance aux effets catastrophiques.

Le choix de conception du système fournissant la position verticale proposé à la figure 14 ci dessous est le suivant:

a. Le système est constitué de deux portions dissimiliaire, primaire et backup (il s'agit du pattern 5 du tableau 4 de l'ARP 4754)) ,
b. La portion primaire du système est constituée de deux portions, l'une dite active, l'autre qui assure une surveillance (pattern 4 du tableau 4 de l'ARP 4754)).

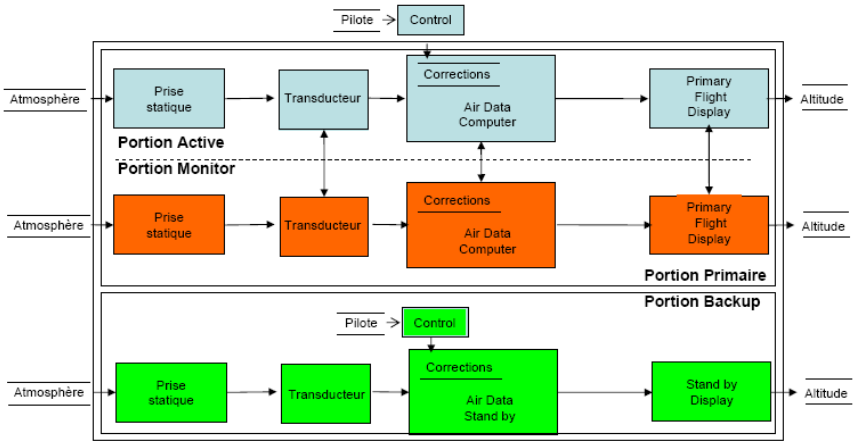

Figure 14. Projet d'architecture robuste à l'information altitude erronée ou perdue

Sous ces hypothèses, l'ARP 4754 nous indique que le DAL de la portion primaire doit être A (P.DAL = A), celui de la partie backup doit être au moins égale à C (B.DAL≥C). Le DAL de la partie active de la portion primaire doit être au moins égal à C (P.A.DAL≥C) tandis que la partie surveillance de la portion primaire doit avoir un DAL égal à A (P.S.DAL=A)

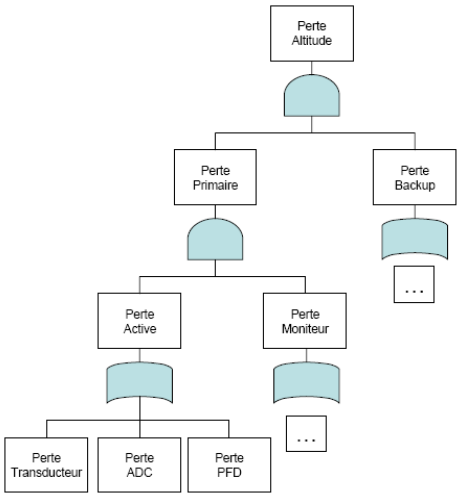

Figure 15. Arbre de défaillance associé à la perte de l'information altitude

De même, le modèle ci-dessus, figure 15, donne un aperçu des représentations d'évaluation de la sûreté qui viennent compléter les représentations logiques et physiques d'un système. Il est réalisé sous l'hypothèse de l'architecture physique présentée à la figure 14.

La validation des exigences de sûreté, comme l'indique la figure 16, s'inscrit exactement dans le cadre général de la validation des exigences (et des hypothèses) et se déroule suivant les mêmes modalités que celles décrites au paragraphe 2-4.

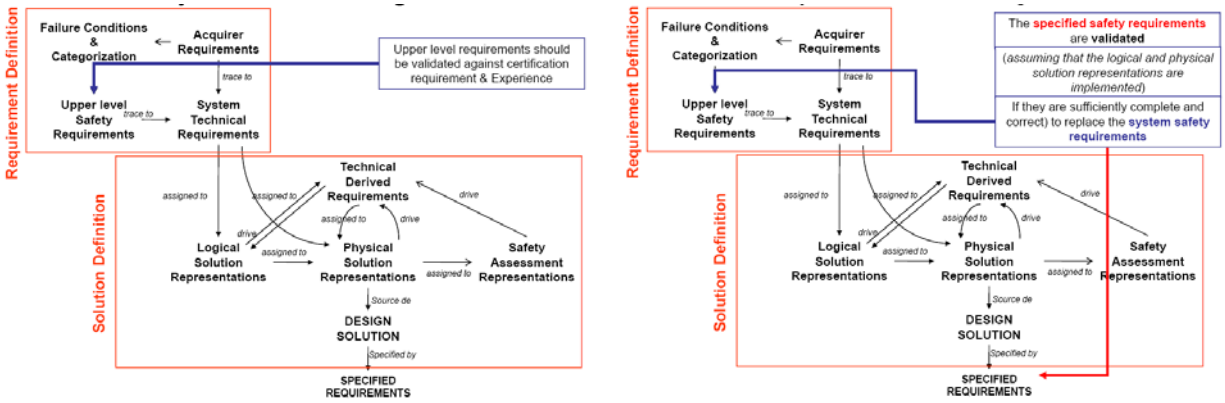

Figure 16. Validation des exigences de sûreté

Tandis que la vérification d'un bloc de construction par rapport à ses exigences de sûreté suit le schéma représenté sur la figure 17.

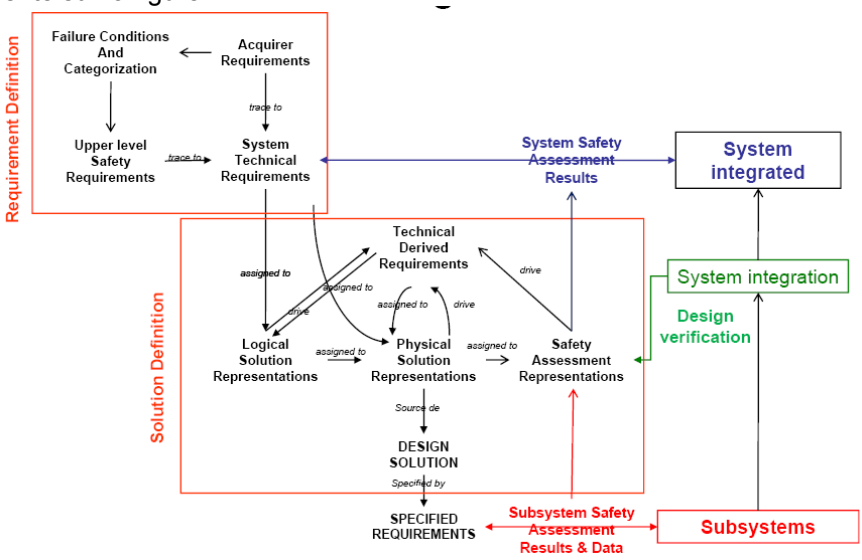

Figure 17. Vérification du bloc vis-à-vis de ses exigences de sûreté

La vérification du système par rapport aux exigences de sûreté s'inscrit exactement dans le cadre général de la vérification des exigences et se déroule suivant les mêmes modalités que celles décrites au paragraphe 2-5.

1. la vérification des sous systèmes est réalisée par rapport aux exigences de sûreté qui leur ont été spécifiées. Elle produit des données et des résultats de sûreté de niveau sous systèmes
2. La vérification de la conformité de l'intégration des sous systèmes réalisés par rapport à la description de conception. La représentativité des modèles d'évaluation de la sûreté par rapport à l'architecture du système réellement intégré est vérifiée.
3. la vérification du système réalisé par rapport aux exigences de sûreté qui lui sont alloué est établie par analyse et calcul en s'appuyant d'une part sur les données ou les résultats d'évaluation de sûreté obtenus au et d'autre part sur le modèles d'évaluation de la sûreté (FTA, DD, FMEA) du bloc de construction.

Le résultat de cette vérification permet d'assurer que les objectifs de sûreté sont tenus ou bien d'identifier des écarts.

Conclusion.

Dans cet article nous avons montré comment il était possible d'étendre le cadre de conception des systèmes complexes proposé par l'EIA 632 de manière à y intégrer les activités de développement et les activités d'évaluation de la sûreté, de satisfaire aux exigences émises par les autorités de certification telles que l'EASA ou la FAA, de répondre à des standards tels que l'ED-79/ARP 4754, l'ED-80/DO-254, l'ED-12/DO-178B.

L'intégration des modèles d'évaluation de la sûreté aux modèles logiques et physiques de l'EIA 632 contribue également à la définition d'un processus d'ingénierie des systèmes aéronautiques basé sur des modèles.
Enfin notre théorie des exigences bien formées pourrait constituer un fondement théorique à une intégration de l'ingénierie des exigences à l'ingénierie des systèmes aéronautiques basée sur des modèles. Des travaux à publier dans les prochains mois pourraient confirmer la fécondité de cette voie, tandis que, selon Sanford Friedenthal [12], elle pourrait être prise en compte dans une future version de SysML.

REFERENCES

[1] AC 25-11A: Advisory Circular, Electronic Flight Deck Displays, FAA, US Department of Transportation, 26 juin 2007, FAA, US Department of Transportation, 25 avril 2006.
[2] AC 29-2C: Advisory Circular, Certification of Transport Category Rotorcraft, FAA, US Department of Transportation, 25 avril 2006.
[3] ANSI/EIA 632: Processes for Engineering a System, GEIA, Arlington, VA, 2003.
[4] ARINC 429: Mark 33 Digital Information Transfer System (DITS), ARINC Specification, AERONAUTICAL RADIO, INC,
[5] ARINC 706-4: Mark 5 Subsonic Air Data System, ARINC Characteristic, AERONAUTICAL RADIO, INC, january 11, 1988,
[7] CS-29 : EASA Specification Certification for Large Rotorcrafts, European Aviation Safety Agency.
[8] ED-12/DO-178B : Software Considerations in Airborne Systems and Equipment Certification, RTCA, 1992,
[9] ED-79/ARP 4754 : Certification considerations for Highly-Integrated or Complex Aircrafts Systems, SAE 1996-11, 1996
[10] ED-80/DO-254 : Software Considerations in Airborne Systems and Equipment Certification, RTCA, 2000
[11] ED-135/ARP 4761 : Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipments, SAE 1996-12, 1996
[12] FRIEDENTHAL Sanford : SysML Information Days, Summary and Wrap-up, OMG Technical Meeting Santa Clara, CA, December 8-11, 2008 (ftp://ftp.omg.org/pub/docs/syseng/08-12-14.pdf)
[13] JACKSON Scott, Systems engineering for commercial aircraft, Ashgate Publisher, 1997
[14] MICOUIN Patrice, Toward a property based requirements theory: System requirements structured as a semilattice, INCOSE Journal of Systems Engineering, Volume 11, Issue 3 (August 2008), John Wiley and Sons Publisher.
[15] MOIR Ian & SEABRIDGE Allan, Civil Avionics Systems, 2003, John Wiley and Sons Publisher.
[16] SAE- AS8002A : Air Data Computer : Minimum Performance Standard, Aerospace Standard SAE International, 1996-09
[17] SPITZER Cary R., Avionics Development and Implementation, 2nd Edition, CRC Press, 2007.
[18] TSO-C10b, Altimeter, Pressure Actuated, Sensitive Type, 1 septembre 1959.
[19] TSO-C106, Air Data Computer, 15 janvier 1988.

BIOGRAPHIE

Patrice MICOUIN: Consultant senior dans le domaine de l'Ingénierie des Systèmes travaille auprès de sociétés telles que DCNS (systèmes navals), Airbus Avionics and Simulation Products (Avionics), Eurocopter (constructeur d'hélicoptères), et le CNES (agence spatiale française). En 2006, il a soutenu à l'Ecole Nationale Supérieure des Arts et Métiers (ENSAM), une thèse de doctorat traitant de la définition et du déploiement d'un processus d'ingénierie de systèmes dans le secteur automobile (illustré par le processus de conception d'une chaîne de traction hybride électrique chez PSA Peugeot Citroën). Il mène ses recherches autour de l'ingénierie des exigences, de l'ingénierie de conception et de la représentation des connaissances au Laboratoire LSIS (UMR CNRS 6168). Patrice Micouin est membre du chapitre AFIS de l'INCOSE, de l'IEEE et de la Design Society.